COS 522 Complexity - Spring 2007 - Final Take Home Exam

- Read these instructions carefully *before* starting to work on the exam. If any of them are not clear, please email me before you start to work on the exam.

- **Schedule:** You can work on this exam in a period of 48 hours of your choice between May 7^{th} to **May 21^{st} 10:00am**. You should type up your exam (preferably using LaTeX) and email it to me by May 21^{st} 10:00 am. *This is a strict deadline.* You may submit the exam earlier. In addition, please submit a hardcopy of the exam to my mailbox.

- **Restrictions , honor code:** You should work on the exam alone. You can use your notes from the class, the homework exercises and their solutions, the textbook and the handouts I gave in class. You can also use any personal summaries and notes of the material that you prepare before starting to work on the exam. *You should not use any other material while solving this exam.* You should write and sign the honor pledge on the hardcopy of the submitted exam (the pledge is "I pledge my honor that I did not violate the honor code during this exam and followed all instructions").

- **Writing:** You should answer all questions *fully*, *clearly* and *precisely*. When describing an algorithm or protocol, state clearly what are the inputs, operation, outputs, and running time. When writing a proof, provide clear statements of the theorem you are proving and any intermediate lemmas or claims.

- **Partial solutions:** If there is a question you can not solve fully, but you can solve a partial/relaxed version or a special case, then please state clearly what is the special case that you can solve, and the solution for this case. You will be given partial credit for such solutions, as long as I feel that this special case captures a significant part of the question's spirit.

- **Quoting results:** You can quote without proof standard mathematical tools such as Chernoff bounds, and concepts from linear algebra (inner product, eigenvalues etc.). However, you should quote the results precisely, and give a reference to the place in the textbook where the result is stated.

- **Clarifications:** I have made an effort to make the questions as clear and unambiguous as possible. In case any clarifications are needed, I will try to be always available by email. You can also email me with your number and good times to call, and I will call you back. If you need me more urgently, you can call me at my cell phone 917-674-6110 between 10am and 10pm eastern time. If there are any unresolved doubts, please write your confusion as part of the answer and maybe you will get partial credit.

Turn the page only when you are ready to start working on the exam.

This exam has a total of 4 questions, each worth 25 points, summing up to 100 points.

Question 1. Prove that if G is an $(n, D, 1-\epsilon)$-graph and G' is a $(D, d, 1-\epsilon')$-graph then the (balanced) *replacement product* $G \circledR G'$ of of G and G' (as defined in Section 16.4.4) is an $(nD, 2d, 1-(\epsilon\epsilon')^4/100)$ graph. (This is implied by Lemma 16.23 but there's actually a bug in the proof of that lemma in the book, since it relied on an inaccurate description of the adjacency matrix of the replacement product.)

Question 2. Prove Theorem 16.25: There exist constants $d \in \mathbb{N}$ and $\lambda < 1$ such that there is a strongly explicit family of d regular λ-expander graphs $\{G_N\}_{N \in \mathbb{N}}$. That is, for every N, G_N is an (N, d, λ)-graph and there is a polynomial-time algorithm A that on input (N, u, i) (represented in binary) where $u \in [N]$ and $i \in [d]$, outputs the index of the i^{th} neighbor of u in G_N. You may use any lemma that has a full proof in the text and also the result of the previous question. See footnote for hint[1]

Question 3. Solve Exercise 16.9. That is, prove that if $k \in \mathbb{N}$ and X is a distribution over $\{0,1\}^n$ with min-entropy at least k (i.e., $\Pr[X = x] \leq 2^{-k}$ for every x), then X is a convex combination of distributions that are uniform over subsets of $\{0,1\}^n$ of size at least 2^k. See footnote for hint[2]

Question 4. Prove the following slightly relaxed version of Lemma 16.34: that if X is a distribution over $\{0,1\}^n$ with min-entropy at least $2k/\delta$ and h is chosen from a pairwise independent hash function family from $\{0,1\}^n$ to $\{0,1\}^k$, then the distribution $h(X) \circ h$ is within statistical distance at most 10δ from $U_k \circ h$ (where $\circ$ denotes concatenation and U_k denotes the uniform distribution over $\{0,1\}^k$).

[1] **Hint:** First show how to teak the construction of the text to obtain such a graph for every N that is of the form $N = c^n$ for some constant c. Then, show that you can use this to obtain a construction of graphs of every size.

[2] **Hint:** you can use Farkas' Lemma (see Note 17.5).